UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

TRACI DIANA JULIN, on behalf of herself and all others similarly situated, **Plaintiff** **v.** **QUEST DIAGNOSTICS INCORPORATED, OPTUM360, LLC and AMERICAN MEDICAL COLLECTION AGENCY, INC.** **Defendants.**	**CASE NO.:** **CLASS ACTION** **COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORY AND INJUNCTIVE RELIEF** **DEMAND FOR JURY TRIAL**

Plaintiff, Traci Diana Julin ("Plaintiff"), individually and on behalf of those similarly situated, brings this class action lawsuit against Quest Diagnostics Incorporated ("Quest"), Optum360, LLC ("Optum") and American Medical Collection Agency, Inc. ("AMCA") (collectively "Defendants") based upon personal knowledge as to herself, and on information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for: failing to properly secure and safeguard protected health information, as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), medical information, and other personally identifiable information (collectively, "PII"); failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members (defined below) that the integrity of their PII had been compromised; and failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members of the nature and scope of the PII that was exposed.

2. On June 3, 2019, Quest publicly announced that approximately two weeks earlier on May 14, 2019, its billing collections vendor AMCA advised Quest of "unauthorized activity on AMCA's web payment page" which compromised the PII of approximately 11.9 million Quest

patients.[1] The exposed PII included "financial information (e.g., credit card numbers and bank account information), medical information and other personal information (e.g., Social Security Numbers)" ("Data Breach"). *Id.* Quest further revealed that the exposure occurred between August 1, 2018, and March 30, 2019.

3. Despite the breadth and sensitivity of the PII that was exposed and the attendant consequences to patients as a result thereof, Defendants failed to disclose the Data Breach for nearly two months from the time it was first discovered, further exacerbating harm to patients. Moreover, to date, Defendants have not disclosed the full extent and nature of the Data Breach, nor offered anything to its patients to address and compensate the harm they have suffered.

4. This Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Patient PII.

5. Defendants disregarded the rights of Plaintiff and Class Members by: intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Patient PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

6. As a result of Defendants' failure to implement and follow basic security procedures, Patient PII is now in the hands of thieves. Plaintiff and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach and will forever be at a heightened risk of identity theft and fraud.

---

[1] Quest Form 8-K filed June 3, 2019 available at https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm (last visited June 5, 2019)

7. Plaintiff, on behalf of all others similarly situated, alleges claims for negligence, invasion of privacy, breach of contract, breach of implied contract, unjust enrichment, breach of fiduciary duty, breach of confidence and violation of New Jersey's Consumer Fraud Act and seeks to compel Defendants to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices to safeguard Patient PII that remains in their custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

8. Plaintiff, Traci Diana Julin is a resident of Lake Mary, Florida and a frequent Quest patient. Ms. Julin suffers from a chronic condition which requires routine testing services, many of which were performed by Quest. Over the past three years, Ms. Julin has retained Quest's laboratory services on at least 17 occasions including the following dates: 5/10/19, 4/11/19, 12/12/17, 10/31/17, 10/26/17, 10/24/17, 6/27/17, 6/2/17, 5/30/17, 5/22/17, 11/11/16, 8/22/16, 6/28/16, 4/19/16, 3/29/16, 10/12/15, and 7/22/15.

9. As a result of the Data Breach, and Defendants' failure to prevent it, Ms. Julin will continue to be at heightened risk for medical fraud, financial fraud, and identity theft along with their attendant damages for years to come.

10. Defendant, Quest Diagnostics Incorporated is a business entity incorporated under the laws of Delaware and headquartered in New Jersey at Three Giralda Farms Madison, 07940. Defendant operates laboratory locations throughout the State of New Jersey, including within Middlesex County with a laboratory location located at 92 Albany Street, Ground Floor, New Brunswick, New Jersey 08901.

11. Defendant, Quest is a leading provider of diagnostic information services and laboratory testing, offering diagnostic testing for conditions as wide ranging as Allergy and Asthma

testing, HIV testing, Ovarian Cancer Screening, Breast Cancer Screening, Celiac Disease Screening, Colorectal Cancer Screening, Hepatitis C testing, Prenatal Health, and Vitamin D testing.[2]

12. Quest maintains a web portal through which patients can interact with the company and provide a range of PII. The website provides: "[t]his Web site can be accessed from the United Stated (sic) and other countries worldwide. Since the laws of each State or country may differ, you agree that the statutes and laws of the State of New Jersey, without regard to any principles of conflicts of law, will apply to all matters relating to the use of this site." [3]

13. Defendant, America Medical Collection Agency, Inc. is a New York corporation headquartered at 4 Westchester Plaza # 110, Elmsford, NY 10523, and claims to be the Nation's leading recovery agency for patient collections managing over $1BN in annual receivables for a diverse client base.

14. Defendant, Optum360, LLC provides billing collections services to the health industry. On information and belief. Optum360 is contracted by Quest to provide billing collections services. The company was incorporated in 2013 and is headquartered in Eden Prairie, Minnesota.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are approximately 11.9 million putative class members, at least some of whom have a different citizenship from Defendants.

16. This Court has jurisdiction over Defendants as Quest is headquartered and operates in this District and Defendants, through their business operations intentionally avail themselves of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

---

[2] Quest Diagnostics, *Diagnostic Testing A-X*, Available at http://www.questdiagnostics.com/home/patients/tests-a-z.html, last accessed June 5, 2019.

[3] Available at http://www.questdiagnostics.com/home/privacy-policy/terms-conditions.html, last visited June 5, 2019.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District. Plaintiff and Class Members received health services from Quest who received and maintained their PII in this District and has caused harm to Plaintiff and Class Members residing in this District.

STATEMENT OF FACTS

A. *The Data Breach*

18. On June 3, 2019, Quest announced in a periodic public filing on Form 8-K and an accompanying press release that highly sensitive PII of 11.9 million of its patients had been improperly exposed over a period of 7 months. The breach occurred on the systems of Quests, billing collections vendor, AMCA. According to the filing, "between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA's system that contained information that AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself." The release further that a broad array of sensitive PII was exposed including "financial information (e.g., credit card numbers and bank account information), medical information and other personal information (e.g., Social Security Numbers)." As announced by Quest on June 3, 2019:

> Quest Diagnostics Statement on the AMCA Data Security Incident
>
> SECAUCUS, N.J., June 03, 2019 -- American Medical Collection Agency (AMCA), a billing collections service provider, has informed Quest Diagnostics that an unauthorized user had access to AMCA's system containing personal information AMCA received from various entities, including from Quest. AMCA provides billing collections services to Optum360, which in turn is a Quest contractor. Quest and Optum360 are working with forensic experts to investigate the matter.
>
> AMCA first notified Quest and Optum360 on May 14, 2019, of potential unauthorized activity on AMCA's web payment page. On May 31, 2019, AMCA notified Quest and Optum360 that the data on AMCA's affected system included information regarding approximately 11.9 million Quest patients. AMCA believes this information includes personal information, including certain financial data, Social Security numbers, and medical information, but not laboratory test results.

> AMCA has not yet provided Quest or Optum360 detailed or complete information about the AMCA data security incident, including which information of which individuals may have been affected. And Quest has not been able to verify the accuracy of the information received from AMCA.
>
> Quest is taking this matter very seriously and is committed to the privacy and security of our patients' personal information. Since learning of the AMCA data security incident, we have suspended sending collection requests to AMCA.
>
> Quest will be working with Optum360 to ensure that Quest patients are appropriately notified consistent with the law.
>
> We are committed to keeping our patients, health care providers, and all relevant parties informed as we learn more.[4]

19. Quest and Optum claimed they first discovered the Data Breach on May 14, 2019, but waited for an additional two weeks before revealing to the Plaintiff and Class Members. Although a specific date was not disclosed, clearly AMCA had been aware of the breach much earlier than that.

B. Defendants' Privacy Practices

20. Quest maintains a Notice of Privacy Practices on its website ("Privacy Practices") which provides in relevant part:

> Quest Diagnostics and its wholly owned subsidiaries (collectively "Quest Diagnostics") are committed to protecting the privacy of your identifiable health information. This information is known as "protected health information" or "PHI." PHI includes laboratory test orders and test results as well as invoices for the healthcare services we provide.
>
> Our Responsibilities

[4] June 3, 2019 Press Release, *Quest Diagnostics Statement on the AMCA Data Security Incident*, available at http://newsroom.questdiagnostics.com/AMCADataSecurityIncident (last visited June 5, 2019)

> **Quest Diagnostics is required by law to maintain the privacy of your PHI.** We are also required to provide you with this Notice of our legal duties and privacy practices upon request. It describes our legal duties, privacy practices and your patient rights as determined by the Health Insurance Portability and Accountability Act (HIPAA) of 1996. We are required to follow the terms of this Notice currently in effect. We are required to notify affected individuals in the event of a breach involving unsecured protected health information. PHI is stored electronically and is subject to electronic disclosure. This Notice does not apply to non-diagnostic services that we perform such as certain drugs of abuse testing services and clinical trials testing services.[5]

21. In addition to the Privacy Practices, Quest maintains a Privacy Policy on its website ("Privacy Policy")[6] which provides, in relevant part:

> **What Personal Information We Collect**
>
> Quest Diagnostics collects your personal information online when you voluntarily provide it to us. If you choose to register online, we ask you to provide limited personal information, such as your name, address, telephone number and/or email address. We also collect information that will allow you to establish a username and password if you would like to do that...
>
> **How We Use Personal Information That We Collect Online**
>
> Internal Uses
>
> We may use your personal information within Quest Diagnostics: (1) to provide you with the services and products you request or that have been ordered and/or requested by your healthcare provider acting on your behalf; (2) to answer questions about our services; billing, payment methods or use of our website; (3) to process or collect payments for our services, (4) to conduct customer surveys; and (5) to contact you about the products and services that we offer.
>
> **Disclosure of Personal Information to Third Parties**

---

[5] Available at http://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html, last visited December 19, 2016. (emphasis added)

[6] Available at: http://www.questdiagnostics.com/home/privacy-policy/online-privacy.html, last visited December 19, 2016.

> We will not disclose any personal information to any third party (excluding our contractors to whom we may provide such information for the limited purpose of providing services to us and who are obligated to keep the information confidential), unless (1) you have authorized us to do so; (2) we are legally required to do so, for example, in response to a subpoena, court order or other legal process and/or, (3) it is necessary to protect our property rights related to this website. We also may share aggregate, non-personal information about website usage with unaffiliated third parties. This aggregate information does not contain any personal information about our users.
>
> **How We Protect Information Online**
>
> We exercise great care to protect your personal information. This includes, among other things, using industry standard techniques such as firewalls, encryption, and intrusion detection.[7]

22. Quest collects and stores an enormous amount of PII which it provides to its vendors and sub-contractors such as Optum and AMCA to further its business. As recipients of sensitive patient PII, Defendants Optum and AMCA are similarly obligated to safeguard the integrity of such data on behalf of Quest patients.

23. Indeed, AMCA boldly states that they are "compliant with all Federal and State Laws and are members of ACA International. We provide our services adhering to the ethical guidelines expected from a National Accounts Receivable Management firm."[8]

24. Consumers place value in data privacy and security, and they consider it when engaging services. Plaintiff and Class Members would not have utilized Quest's services had they known that Defendants did not take all necessary precautions to secure the personal data given to them by consumers.

---

[7] Emphasis added.

[8] Available at http://amcaonline.com/about.php (last visited June 5, 2019)

25. Defendants failed to disclose their negligent and insufficient data security practices and consumers relied on or were misled by this omission into using Defendants services.

C. Defendants were aware that the Medical Industry was a Favorite Target of Hackers

26. The technology and medical industry are rife with similar examples of hackers targeting users' Private Information, including Anthem[9], Premera[10], and St. Joseph Health System[11] among others, all of which predate the time-frame Defendants have identified regarding the Data Breach at issue in the present lawsuit.

27. Indeed, as early as 2014, the FBI alerted healthcare stakeholders that they were the target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)".[12]

Defendants' failure to heed this warning and to otherwise maintain adequate security practices resulted in this Data Breach

D. <u>The Value of Personally Identifiable Information</u>

---

[9] Los Angeles Times, *Anthem is warning consumers about its huge data breach. Here's a translation*, March 6, 2015. Available at http://www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html, last accessed December 19, 2016.

[10] New York Times, *Premera Blue Cross Says Data Breach Exposed Medical Data*, March 17, 2015. Available at http://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html?_r=0, last accessed December 19, 2016.

[11] Napa Valley Register, *St. Joseph Health System sued for patient data breach*, April 9, 2012. Available at http://napavalleyregister.com/news/local/st-joseph-health-system-sued-for-patient-data-breach/article_948c0896-82a3-11e1-bed6-0019bb2963f4.html, last accessed December 19, 2012.

[12] Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014. Available at http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820, last accessed December 19, 2016.

28. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[13] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[14] The FTC acknowledges that identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[15]

29. PII is such a valuable commodity that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[16] Indeed, as a result of large-scale data breaches, Social Security numbers, healthcare information, and other PII have been made publicly available to identity thieves and cybercriminals.

30. Professionals tasked with trying to stop fraud and other misuse acknowledge that PII has real monetary value in part because criminals continue their efforts to obtain this data.[17] According to the Identity Theft Resource Center, 2017 saw 1,579 data breaches, representing a 44.7 percent increase over the record high figures reported a year earlier.[18] The Healthcare sector had the

---

[13] 17 C.F.R § 248.201 (2013).

[14] *Id.*

[15] *Guide for Assisting Identity Theft Victims*, FTC (Sep. 2013), *available at*: https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (the "FTC Guide")(last visited April 21, 2019).

[16] FTC Guide, *supra* n.9.

[17] *Data Breaches Rise as Cybercriminals Continue to Outwit IT, CIO Magazine*, https://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html (last visited January 23, 2019).

[18] *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches, (last visited January 23, 2019).

second largest number of breaches among all measured sectors and the highest rate of exposure per breach.[19]

31. Healthcare related data is among the most sensitive, and personally consequential when compromised. A report focusing on health-care breaches found that the "average total cost to resolve an identity theft-related incident…came to about $20,000," and that the victims were forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage. [20] Almost 50 percent of the victims lost their health care coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.[21]

32. Defendants knew the importance of safeguarding patient PII entrusted to them and of the foreseeable consequences if their data security systems were breached, including the significant costs that would be imposed on affected patients as a result of a breach.

E. Defendants Acquire, Collect, and Store Plaintiff's and Class Members' PII

33. Defendants acquire, collect, store, and maintain a massive amount of protected health related information and other personally identifiable data on their patients.

34. As a condition of engaging in health services, Quest requires that their customers entrust them with highly sensitive personal information.

35. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the Class Members' PII, Quest along with its vendors and sub-contractors assumed legal and equitable duties

---

[19] Identity Theft Resource Center, 2018 End -of-Year Data Breach Report. Available at https://www.idtheftcenter.org/2018-data-breaches/ (last visited April 19, 2019).

[20] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited April 21, 2019)

[21] *Id.*

to those individuals and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII from disclosure.

36. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and the Class Members, as current and former patients, relied on the Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

37. Defendants acknowledge, as they must, their obligation to maintain the privacy of patient PII entrusted to them. (e.g. "Quest is taking this matter very seriously and is committed to the privacy and security of our patients' personal information").[22]

F. Defendants' Conduct Violates HIPAA and Industry Standard Practices

38. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendants left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

39. Defendants' Breach resulted from a combination of insufficiencies that indicate Defendants failed to comply with safeguards mandated by HIPAA regulations and industry standards. Quest's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to adequately catalog the location of patients/customers', including Plaintiff's and Class Members', digital information;

d. Failing to properly encrypt Plaintiff's and Class Members' PII;

e. Failing to ensure the confidentiality and integrity of electronic protected health information Defendants create, receive, maintain, and transmit in violation of 45 CFR 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information

[22] http://newsroom.questdiagnostics.com/AMCADataSecurityIncident

systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

h. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

i. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

j. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 CFR 164.306(a)(94);

l. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*;

m. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45 CFR 164.308(a)(5); and

n. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

G. Defendants Failed to Maintain the Confidentiality of Plaintiff and Class Members' Private Health Information

40. Defendant had a duty to maintain the confidentiality of Plaintiff and Class Members' PII

41. Defendants' duties included ensuring Plaintiff and Class Members' electronically protected PII was not made available or disclosed to unauthorized third persons or processes.

42. Defendants' duties also included protecting against reasonably anticipated threats or hazards to the security of Plaintiff and Class Members' Private Health Information.

43. Defendants failed to adequately protect Plaintiff and Class Members' PII from the reasonably anticipated threat of hackers accessing their systems and the PII contained therein.

44. As a result of the Defendants' failure to protect against reasonably anticipated threats, Plaintiff and the Class Members PII was improperly made available and disclosed to third persons.

45. Plaintiff and Class Members have a privacy right in their medical records, medical information, financial information, and other PII.

46. As a result of Defendants' failure to maintain the confidentiality of Plaintiff and Class Members' PII, Plaintiff and Class Members suffered an injury through their loss of privacy.

H. Plaintiff and Class Members Suffered Damages

47. The ramifications of Defendants' failure to keep Patients' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

48. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendants who did not obtain Plaintiff's or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

49. The Data Breach was a direct and proximate result of Defendants' failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

50. Defendants had the resources necessary to prevent the Breach but neglected to adequately invest in data security measures, despite their obligations to protect Patient data.

51. Had Defendants remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into their systems and, ultimately, the theft of PII.

52. As a direct and proximate result of Defendants' wrongful actions and inaction, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[23]

53. Despite professing to "taking this matter very seriously" and being "committed to the privacy and security of [] patients' personal information," neither Quest, nor the other Defendants have offered patients anything to address the harm caused by them.

54. As a result of the Defendants' failure to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal and medical information being placed in the hands of criminals;

d. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

---

[23] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited April 19,2019).

e. The continued risk to their PII, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fails to undertake appropriate measures to protect the PII in their possession; and

f. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

g. Ascertainable losses in the form of deprivation of the value of their Personal Identifying Information and Private Health Information, for which there is a well-established national and international market;

h. Overpayments for products and services in that a portion of the price paid for such products and services by Plaintiff and Class members was for the costs of reasonable and adequate safeguards and security measures that would protect users' Private Information, which Defendants did not implement and, as a result, Plaintiff and Class Members did not receive what they paid for and were overcharged.

55. In addition to a remedy for the economic harm, Plaintiff and the Class maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

56. Plaintiff seeks relief on behalf of herself and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons whose PII was exposed to unauthorized third parties as a result of the Data Breach announced on June 3, 2019 ("Class").[24]

[24] PII includes, but is not limited to, protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), medical information, and other personally identifiable information including, without limitation to, names, health plan identification numbers,

57. Excluded from the Class are Defendants and any of its affiliates, parents or subsidiaries; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned, their immediate families, and court staff.

58. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

59. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3), and (c)(4).

60. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Patients affected in the Data Breach is unknown, upon information and belief, it is in excess of 11.9 million, and therefore meets the numerosity requirement of 23(a)(1).

61. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Defendants had a duty to protect patient PII;

b. Whether Defendants knew or should have known of the susceptibility of their systems to a data breach;

c. Whether Defendants' security measures to protect their systems were reasonable in light of the FTC data security recommendations, and best practices recommended by data security experts;

d. Whether Defendants were negligent in failing to implement reasonable and adequate security procedures and practices;

---

dates of birth, gender, address, health plan names, health plan eligibility dates, insurance types and coverage information.

e. Whether Defendants' failure to implement adequate data security measures allowed the breach of its data systems to occur;

f. Whether Defendants' conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unlawful exposure of the Plaintiff's and Class Members' PII;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Defendants' failure to reasonably protect its systems and data network; and,

h. Whether Plaintiff and Class Members are entitled to relief.

62. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff is a patient whose PII was exposed in the Data Breach. Plaintiff's damages and injuries are akin to other Class members, and Plaintiff seeks relief consistent with the relief sought by the Class.

63. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class he seeks to represent; is committed to pursuing this matter against Defendants to obtain relief for the Class; and has no conflicts of interest with the Class. Moreover, Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation of this kind. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

64. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to an individual plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by

each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

65. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

66. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the public of the Data Breach;
b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
c. Whether Defendants' security measures to protect its data systems were reasonable in light of FTC data security recommendations, and other best practices recommended by data security experts;
d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;
e. Whether Defendants failed to take commercially reasonable steps to safeguard patient PII; and
f. Whether adherence to FTC data security recommendations and measures recommended by data security experts would have reasonably prevented the data breach.

67. Finally, all members of the proposed Classes are readily ascertainable. Defendants have access to patient names and addresses affected by the Data Breach. Using this information, Class members can be identified and ascertained for the purpose of providing notice.

FIRST CAUSE OF ACTION
NEGLIGENCE
(AS TO ALL DEFENDANTS)

68. Plaintiff restates and realleges paragraphs 1 through 67 above as if fully set forth herein.

69. As a condition of receiving services, Plaintiff and Class Members were obligated to provide Defendants with their PII.

70. Plaintiff and the Class Members entrusted their PII to Quest with the understanding that Quest and its vendors and sub-contractors would safeguard their information.

71. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

72. Defendants had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing the Defendants' security protocols to ensure that Plaintiff's and Class Members' information in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on cybersecurity measures regarding the security of patient information.

73. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew of or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, the current cyber scams being perpetrated and that it had inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiff and the Class.

74. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendants' misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included its decision not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiff and Class Members.

75. Plaintiff and the Class Members had no ability to protect their PII that was in Defendants' possession.

76. Defendants were in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

77. Defendants had a duty to have proper procedures in place to prevent the unauthorized dissemination Plaintiff and Class Members' PII.

78. Defendants have admitted that Plaintiff's and Class Members' PII was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

79. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding the Plaintiff's and Class Members' PII while it was within the Quest's possession or control.

80. Defendants improperly and inadequately safeguarded Plaintiff's and Class Members' PII in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

81. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' PII.

82. Defendants, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiff and Class Members the existence, and scope of the Data Breach.

83. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII would not have been compromised.

84. There is a temporal and close causal connection between Defendants' failure to implement security measures to protect the PII of current and former patients and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class.

85. As a result of Defendants' negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

SECOND CAUSE OF ACTION
INVASION OF PRIVACY
(AS TO ALL DEFENDANTS)

86. Plaintiff restates and realleges paragraphs 1 through 67 above as if fully set forth herein.

87. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

88. Defendants owed a duty to patients, including Plaintiff and Class Members, to keep their PII contained as a part thereof, confidential.

89. Defendants failed to protect patient PII by allowing unauthorized third parties to gain unfettered access to Plaintiff's and Class Members' PII.

90. The unauthorized release of PII, especially the type related to personal health information, is highly offensive to a reasonable person.

91. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendants as part of their use of Quests' services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

92. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

93. Defendants acted with a knowing state of mind when they permitted the Data Breach because they were with actual knowledge that their information security practices were inadequate and insufficient.

94. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

95. As a proximate result of Defendants' acts and omissions, Plaintiff's and Class Members' PII was disclosed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

96. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendants can be viewed, distributed, and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

THIRD CAUSE OF ACTION
BREACH OF CONTRACT
(AS TO QUEST ONLY)

97. Plaintiff restates and realleges paragraphs 1 through 67 above as if fully set forth herein.

98. Plaintiff and Class Members received medical services from Defendant Quest, and in so doing provided their PII.

99. The contract for these services as between Plaintiff and Class Members and Quest was supported by consideration in many forms, including the payment of monies for medical services (e.g., laboratory testing services).

100. Plaintiff and Class Members performed pursuant to these contracts and satisfied all conditions, covenants, obligations, and promises of the agreements.

101. Under these contracts, Defendant Quest was obligated, as outlined in the Notice of Privacy Practices and Privacy Policy, to maintain the confidentiality of Plaintiff and Class Member's PII.

102. Quest's failure to maintain the confidentiality of Plaintiff and Class Members PII was a breach of Quest's contractual obligations as outlined in the Notice of Privacy Practices.

103. By failing to adequately secure Plaintiff and Class Member's PII, Plaintiff and Class Members did not receive the full benefit of the bargain, and instead received services that were less valuable than described in the contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in value between what was promised and what Quest ultimately provided.

104. As a result of Quest's breach of contract, Plaintiff and Class Members have suffered actual damages resulting from the theft of their PHI and PII and remain at imminent risk of suffering additional breaches in the future.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(AS TO ALL DEFENDANTS)

105. Plaintiff restates and realleges paragraphs 1 through 67 above as if fully set forth herein.

106. Plaintiff and Class Members were required to provide their PII, including names, addresses, dates of birth, social security numbers, credit card, and bank information, among other related information to Defendants as a condition of their use and or as a result of using and paying for Quest's services.

107. Plaintiff and Class Members paid money to Defendants in exchange for services, implicit in which were Defendants' promises to protect patient PII from unauthorized disclosure.

108. In their written privacy policies, Defendants promised Plaintiff and Class Members that they would only disclose protected health information and other PII under certain circumstances, none of which relate to the Data Breach, and would otherwise comply with applicable state and federal laws.

109. Defendants each promised and were otherwise obligated to comply with HIPAA standards and to make sure that Plaintiff's and Class Members' protected health information and other PII would remain protected.

110. Implicit in the agreement between the Defendants' patients, including Plaintiff and Class Members, to provide protected health information and other PII, and Defendants' acceptance of such protected health information and other PII, were Defendants' obligation to use the PII of patients for business purposes only, take reasonable steps to secure and safeguard that protected health information and other PII, and not make unauthorized disclosures of the protected health information and other PII to unauthorized third parties.

111. Further, implicit in the agreement, Defendants was obligated to provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their protected health information and other PII.

112. Without such implied contracts, Plaintiff and Class Members would not have provided their protected health information and other PII to Defendants.

113. Defendants had an implied duty to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses.

114. Additionally, Defendants implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

115. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendants; however, Defendants did not.

116. Defendants breached the implied contracts with Plaintiff and Class Members by:

a. failing to reasonably safeguard and protect Plaintiff and Class Members' PII, which was compromised as a result of the Data Breach;

b. failing to comply with their obligations to abide by HIPAA;

c. failing to ensure the confidentiality and integrity of electronic protected health information Defendants created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1);

d. failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii); and

g. failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
(AS TO ALL DEFENDANTS)

117. Plaintiff restates and realleges paragraphs 1 through 67 above as if fully set forth herein.

118. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they purchased medical services from Defendants and in so doing provided Defendants with their PII. In exchange, Plaintiff and Class Members should have received from Defendants the services that were the subject of the transaction and have their PII protected with adequate data security.

119. Defendants knew that Plaintiff and Class Members conferred a benefit on Defendants and accepted and have accepted or retained that benefit. Defendants profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

120. The amounts Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendants' network and the administrative costs of data management and security.

121. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

122. Defendants failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

123. Defendants acquired the PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

124. If Plaintiff and Class Members knew that Defendants would not secure their PII using adequate security measures, they would not have engaged in transactions with Defendants.

125. Plaintiff and Class Members have no adequate remedy at law.

126. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants' fail to undertake appropriate and adequate measures to protect the PII of patients and in their continued

possession; (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (viii) the diminished value of Defendants' services they received.

127. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

128. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

SIXTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(AS TO ALL DEFENDANTS)

129. Plaintiff restates and realleges paragraphs 1 through 67 above as if fully set forth herein.

130. In light of the special relationship between Defendants and their Patients, whereby Defendants became guardians of Plaintiff's and Class Members' highly sensitive, confidential, personal, financial information, and other PII, Defendants became fiduciaries created by their undertaking and guardianship of the PII, to act primarily for the benefit of their Patients, including Plaintiff and Class Members, for: 1) the safeguarding of Plaintiff and Class Members' PII; 2) timely notify Plaintiff and Class Members' of a data breach or disclosure; and 3) maintain complete and accurate records of what and where Defendants' patients' information was and is stored.

131. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their patients' relationship, in particular, to keep secure the PII of their patients.

132. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to diligently investigate the Data Breach to determine the number of Class Members affected in a reasonable and practicable period of time.

133. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' protected health information and other PII.

134. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

135. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendants created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

136. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

137. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

138. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

139. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

140. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

141. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by their workforce in violation of 45 CFR 164.306(a)(94).

142. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, et seq.

143. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45 CFR 164.308(a)(5).

144. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

145. Defendants breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

146. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect

Patient PII in their continued possession; (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (viii) the diminished value of Defendants' services they received.

147. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SEVENTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(AS TO ALL DEFENDANTS)

148. Plaintiff restates and realleges paragraphs 1 through 67 above as if fully set forth herein.

149. At all times during Plaintiff's and Class Members' interactions with Defendants, Defendants was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' protected health information and other PII that Plaintiff and Class Members provided to Defendants.

150. As alleged herein and above, Defendants' relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' protected health information and other PII would be collected, stored, and protected in confidence, and would not be disclosed the unauthorized third parties.

151. Plaintiff and Class Members provided their respective protected health information and PII to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the protected health information and other PII to be disseminated to any unauthorized parties.

152. Plaintiff and Class Members also provided their respective protected health information and PII to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect that protected health information and other PII from unauthorized disclosure, such as following basic principles of encryption and information security practices.

153. Defendants voluntarily received in confidence Plaintiff's and Class Members' protected health information and other PII with the understanding that protected health information and other PII would not be disclosed or disseminated to the public or any unauthorized third parties.

154. Due to Defendants' failure to prevent, detect, avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class Members' protected health information and other PII, Plaintiff's and Class Members' protected health information and PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

155. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiff and Class Members have suffered damages.

156. But for Defendants' disclosure of Plaintiff's and Class Members' protected health information and other PII in violation of the parties' understanding of confidence, their protected health information and other PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' protected health information and other PII, as well as the resulting damages.

157. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and Class Members' protected health information and other PII. Defendants knew their computer systems and technologies for accepting and securing Plaintiff's and Class Members' protected health information and other PII had numerous security vulnerabilities because Defendants failed to observe even basic security practices necessary to prevent fraudulent provider accounts from being created.

158. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (v) lost opportunity costs associated with

effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover identity theft; (vi) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Patient PII in their continued possession; (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (viii) the diminished value of Defendants' services they received.

159. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

EIGHTH CAUSE OF ACTION
VIOLATION OF THE NJ CONSUMER FRAUD ACT, *N.J.S.A.* 56:8-1, *ET SEQ.*
(AS TO ALL DEFENDANTS)

160. Plaintiff restates and realleges Paragraphs 1 through 67 as if fully set forth here.

161. Plaintiff and the Class bring these claims against Defendant under the New Jersey Consumer Fraud Act.

162. Defendants sell "merchandise" as defined by the New Jersey Consumer Fraud Act by offering health services to the public.

163. Defendants engaged in unconscionable and deceptive acts and practices, misrepresentation and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of their services in violation of N.J.S.A. 56:8-2, including by not limited to the following:

a. Misrepresenting material facts, pertaining to their services to consumers by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Class Members' PII from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts by representing to Plaintiff and Class members that they did and would continue to comply with the relevant industry data security standards, state law and federal law with regard to the protection of Plaintiff and Class Members' PII;

c. Defendants knowingly omitted, suppressed and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and the Class Members' PHI and PII with the intent that Plaintiff and the Class Members would rely on the omission, suppression, and concealment;

d. Defendants engaged in unconscionable and deceptive acts and practices by failing to disclose the Data Breach to Plaintiff and Class Members in a timely and accurate manner in violation of N.J.S.A. 56:8-163(a);

164. As a direct and proximate result of Defendants' unconscionable or deceptive acts and practices, Plaintiff and Class Members suffered an ascertainable loss in money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PII.

165. Plaintiff and Class members are therefore entitled to injunctive relief, equitable relief, actual damages, treble damages, and attorneys' fees and costs pursuant to N.J.S.A. 56:8-19.

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, respectfully requests the following relief:

a. An Order certifying this case as a class action;

b. An Order appointing Plaintiff as the class representative;

c. An Order appointing undersigned counsel as class counsel;

d. A mandatory injunction directing the Defendants to hereinafter adequately safeguard the Class' PII by implementing improved security procedures and measures;

e. An award of damages;

f. An award of costs and expenses;

g. An award of attorneys' fees; and

h. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial as to all issues so triable by a jury.

Dated: June 5, 2019

/s/ James A. Barry
James A. Barry, Esq.
jbarry@lockslaw.com
LOCKS LAW FIRM, LLC
801 N. Kings Highway
Cherry Hill, NJ 08034
Tel: (856) 663-8200

John A. Yanchunis, Esq.
jyanchunis@forthepeople.com
Patrick Barthle, Esq.
pbarthle@forthepeople.com
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel: (813) 223-5505
(To be admitted *Pro Hac Vice*)

Michael A. Galpern, Esq.
mgalpern@lawjw.com
JAVERBAUM WURGAFT HICKS KAHN WIKSTROM AND SININS, P.C.
1000 Haddonfield-Berlin Road, Suite 203
Voorhees, NJ 08043
Tel: (856) 596-4100

Jared Michael Lee, Esq.
Florida Bar #: 0052284
Jared@JacksonLeePA.com
Jackson Lee | PA
1991 Longwood Lake Mary Rd
Longwood, FL 32750
Tele: (407) 477-4401
(To be admitted *Pro Hac Vice*)